Commun Nonlinear Sci Numer Simulat 19 (2014) 4094–4104

Contents lists available at ScienceDirect

Commun Nonlinear Sci Numer Simulat

journal homepage: www.elsevier.com/locate/cnsns

An efficient self-adaptive model for chaotic image encryption algorithm

Xiaoling Huang [a], Guodong Ye [b,*]

[a] College of Science, Guangdong Ocean University, Zhanjiang 524088, Guangdong, China
[b] Department of Electronic Engineering, City University of Hong Kong, 83 Tat Chee Avenue, Kowloon Tong, Hong Kong

ARTICLE INFO

Article history:
Received 27 November 2013
Received in revised form 10 April 2014
Accepted 16 April 2014
Available online 24 April 2014

Keywords:
Encryption algorithm
Self-adaptive method
Permutation
Chaotic systems

ABSTRACT

In this paper, an efficient self-adaptive model for chaotic image encryption algorithm is proposed. With the help of the classical structure of permutation-diffusion and double simple two-dimensional chaotic systems, an efficient and fast encryption algorithm is designed. However, different from most of the existing methods which are found insecure upon chosen-plaintext or known-plaintext attack in the process of permutation or diffusion, the keystream generated in both operations of our method is dependent on the plain-image. Therefore, different plain-images will have different keystreams in both processes even just only a bit is changed in the plain-image. This design can solve the problem of fixed chaotic sequence produced by the same initial conditions but for different images. Moreover, the operation speed is high because complex mathematical methods, such as Runge–Kutta method, of solving the high-dimensional partial differential equations are avoided. Numerical experiments show that the proposed self-adaptive method can well resist against chosen-plaintext and known-plaintext attacks, and has high security and efficiency.

1. Introduction

In a modern society, we are processing more and more digital information through electronic equipments such as computers, notebooks, iPhone, iPad, and so on. Among the information sources, digital is one of the most important information, which it can let us understand the content directly. Thus, many images are transmitted over public network every day. However, for some private images, we do not want them to be accessed by unauthorized persons. Obviously, a simple and direct way is to perform encryption on them, so that they can only be decrypted correctly with the correct key. As a result, how to efficiently provide security protection to these secret images has become an urgent issue [1]. However, different from text encryption, images have their intrinsic properties such as bulky data capacity, high redundancy, and high correlation between image pixels [2], traditional techniques (for example, AES and IDEA) are not suitable for real-time encryption of images [3].

To meet the challenge of image protection, there are many schemes [4–6] proposed in recent years. Among them, the chaos-based encryption algorithms [6–15] have shown good efficiency. Maybe we should attribute this success to the characteristics of chaotic system itself such as parameter setting, random behavior, and sensitivity to initial condition. Normally, we adopt the classical permutation-diffusion architecture. This means that the whole encryption process is divided into two stages, i.e., permutation (In this stage, we just shuffle the pixels in the plain-image by some invertible mapping) and diffusion

* Corresponding author. Tel.: +852 34429917.
E-mail address: guodongye@gmail.com (G. Ye).

http://dx.doi.org/10.1016/j.cnsns.2014.04.012
1007-5704/

(Pixel values of the permuted image will be further changed by some chaotic sequence and operation in this stage). To achieve high security, the encryption algorithm should have the ability to let a tiny change in any pixel of the plain-image or any small changes in initial condition resulting in an absolutely different cipher-image [16].

Currently, the low security defect is found in some image encryption algorithms. In [17], Zhu proposed an encryption scheme with two rounds of diffusion only, the chaotic sequence was generated by a four-dimensional hyperchaotic system with four given initial conditions $x_0,\ y_0$, z_0, and w_0. Then the method did a preprocessing for the iterated values from the chaotic system to make a better statistical performance. After that, the chaotic sequence was used for diffusion. However, Li et al. [18] analyzed the security of [17] and suggested a cryptanalysis method known-plaintext. They pointed out that the secret keys, which are used, could be found when two pairs of known plain-image and cipher-images are available [18]. A colour image encryption algorithm was introduced in [19], which used only the Logistic map to generate the chaotic sequence with given initial conditions a, x_0 and a_1, y_0. The iterated chaotic values were used for pixel scrambling and diffusion. Arroyo et al. [20] successfully cryptanalyzed this scheme through a chosen-plaintext attack. The drawbacks of the cryptosystem were also analyzed in detail in two aspects [20]: (1) Small key space, and (2) Low sensitivity to the plain-image.

In this paper, we propose a new image encryption algorithm which possesses the self-adaptive feature. In the permutation stage, the chaotic sequence for the circular shuffling is generated dependent on the plain-image. It solves the key-dependent only problem found in most of the existing algorithms. The keystreams for different plain-images are not identical, which enhances the resistance to known- and chosen-plaintext attacks. Furthermore, in the diffusion, the permuted image is divided into blocks. We choose the last block to update the initial conditions of the chaotic system. As a result, the keystream for diffusion is also dependent on the image. Two mathematical models are established for updating the initial conditions of the chaotic system. Fortunately, with just one round of iteration, the system can nearly reach the required security level.

The rest of this paper is organized as follows, the proposed self-adaptive image encryption algorithm is described in Section 2. Two updating mathematical models are established for the initial conditions of the system. Section 3 gives the numerical experiments using our algorithm. The performance analyses performed in Section 4 demonstrate the security and the efficiency. Finally, some conclusions are drawn in Section 5.

2. The design of self-adaptive image encryption algorithm

2.1. Chaotic system

We know that 1D Logistic map (given by (1)) is a simple chaotic map and has been widely employed in many image encryption algorithms [7,8,21].

$$x_{i+1} = \mu x_i(1 - x_i),\ i = 0, 1, 2, \ldots. \tag{1}$$

When $3.56994 < \mu \leqslant 4$, the system will become chaotic. However, it may lead to insecure encryption algorithm due to small key space and limited number of control parameters. A better way to use is to find a high-dimensional chaotic system which possesses a large key space.

2D Logistic map [8], an extension of the 1D one, is given by following Eq. (2).

$$\begin{cases} x_{i+1} = \mu_1 x_i(1 - x_i) + \gamma_1 y_i^2 \\ y_{i+1} = \mu_2 y_i(1 - y_i) + \gamma_2(x_i^2 + x_i y_i) \end{cases} \tag{2}$$

If we let $2.75 < \mu_1 \leq 3.4, 2.7 < \mu_2 \leq 3.45,\ 0.15 < \gamma_1 \leq 0.21,\ 0.13 < \gamma_2 \leq 0.15$, system (2) will exhibit a chaotic state [8]. Here, the iterated values $x_i, y_i \in (0, 1],\ i = 0, 1, 2, \ldots$.

The generalized Arnold map [10], another 2D chaotic map, can be expressed into the following form (3) with $a > 0, b > 0$ as two integer control parameters.

$$\begin{cases} \overline{x}_{i+1} = \overline{x}_i + a\overline{y}_i \ mod\, 1 \\ \overline{y}_{i+1} = b\overline{x}_i + (1 + ab)\overline{y}_i \ mod\, 1 \end{cases} \tag{3}$$

where $\overline{x}_i,\ \overline{y}_i \in (0, 1),\ i = 0, 1, 2, \ldots$. Since the largest Lyapunov characteristic exponent of system (3) is $\lambda = 1 + \frac{ab + \sqrt{a^2b^2 + 4ab}}{2}$, which is always bigger than one, the map is a chaotic system for any positive a and b [10]. Figs. 1 and 2 show respectively, the chaotic behavior of 2D Logistic map (with $\mu_1 = 3.25$, $\mu_2 = 3.17,\ \gamma_1 = 0.204,\ \gamma_2 = 0.142,\ x_0 = 0.304$, and $y_0 = 0.137$) and the generalized Arnold map (with $a = 2,\ b = 1,\ \overline{x}_0 = 0.225$, and $\overline{y}_0 = 0.409$). In this paper, these chaotic systems are used in the encryption algorithm. More about the properties of these two chaotic systems can be found in references [8,10].

2.2. Self-adaptive model for permutation

Permutation is an operation of exchange the positions of the image pixels, of which can disturb and reduce the high correlation exist in the plain-image pixels. There are many methods to implement the permutation function, for example, Toral automorphism [22], Arnold cat map [23], S-box shuffling [24], Standard map [25]. However, they only consider a